The Role of Compliance Requirements in IT Governance Implementation: An Empirical Study Based on COBIT 2019

Tim Huygh
Open Universiteit,
Heerlen, The Netherlands
Tim.huygh@ou.nl

Dirk Steuperaert
University of Antwerp,
Antwerp, Belgium
Dirk.steuperaert@uantwerpen.be

Steven De Haes
University of Antwerp,
Antwerp, Belgium
Steven.dehaes@uantwerpen.be

Anant Joshi
Maastricht University,
Maastricht, The Netherlands
A.joshi@maastrichtuniversity.nl

Abstract

Rooted in the conformance perspective of IT governance, this paper sets out to research the role of compliance requirements in IT governance implementation, and to shed light on what aspects (i.e., processes) of IT governance are important under different levels of compliance requirements. Based on a large and diverse sample of organizations (N=2566), our results indicate that IT governance implementation level (over five different process domains) consistently goes up with increasing compliance requirements, and that these jumps in IT governance implementation levels are always statistically significant. Moreover, we identify the IT governance processes that are of primary importance for each level of compliance requirements.

1. Introduction

The reality of digital transformation and its widespread impact on organizations, and society at large, are well-known by now [1]. Nevertheless, the recent COVID-19 pandemic even accelerated the digitalization of (certain aspects of) organizations, due to specific challenges and opportunities, for instance in the context of supply chains, and information sharing and collaboration [2]. While digital transformation in general, and the adoption of digital technologies in specific, opens up a wide variety of opportunities and positive outcomes, there are also potentially undesirable issues associated with it, mostly related to security and privacy [1]. As a result, different stakeholders (e.g., customers, employees, investors, business partners, and regulators) are concerned about the security and privacy of organizations' information and technology [3].

An important aspect in this context is the legal and regulatory environment of organizations, in which legal and political actors act to change laws and regulations that apply to these organizations. This often happens in response to certain trigger events or trends. A classic example is the Sarbanes-Oxley (SOX) act of 2002, which was introduced in response to several high profile corporate scandals (e.g., Enron) [4, 5]. In recent years, security and privacy related issues have received ample attention by regulators (e.g., the EU's General Data Protection Regulation, or Brazil's Lei Geral de Proteção de Dados). As a result, organizations certainly need to be aware of what happens in their legal and regulatory environments to be able to manage compliance, avoiding non-compliance and the undesirable effects that are associated with it (e.g., financial, reputational) [6].

Extant literature asserts that the monitoring of changes in the legal and regulatory environment, and ensuring regulatory compliance, is an important attention point in the context of IT governance [7, 8]. This is referred to as the 'conformance' perspective of IT governance [9]. As such, an appropriate IT governance approach is required to ensure regulatory compliance, and an organization's compliance requirements may have an influence on (the appropriateness of) its IT governance approach. However, empirical research on the role of compliance requirements in IT governance implementation is not available and it remains largely unclear what aspects (e.g., processes) of IT governance are important to enable this 'conformance' perspective, and as such enabling regulatory compliance in an ever-changing legal and regulatory environment. In response, the present research aims to investigate the role of compliance requirements in IT governance implementation. More specifically, this paper empirically investigates if organizations with different compliance requirements exhibit differences at the way

URI: https://hdl.handle.net/10125/80146
978-0-9981331-5-7

in which IT governance is implemented. And, if so, how these differences manifest themselves.

2. Theoretical background

2.1. The legal and regulatory environment and compliance

With the digitalization of the global economy, security and privacy related issues are increasingly on the agenda of organizational stakeholders (e.g., customers, employees, investors, business partners, and regulators) [1, 3]. In this context, organizations need to be aware of their legal and regulatory environment, in which legal and political actors act to change laws and regulations, to which organizations need to ensure compliance. An organization's legal and regulatory environment is often complex, with compliance challenges generated by the Sarbanes-Oxley Act, data protection and information privacy legislation (e.g., General Data Protection Regulation), and ethics and integrity regulations [10, 11]. Moreover, popular digital technologies like cloud computing may be a threat to compliance because of its distributed nature, resulting in increasing compliance pressures [12]. On April 21st, 2021, the European Commission released their *"Proposal for a Regulation laying down harmonised rules on artificial intelligence"*, proposing the first ever legal framework on artificial intelligence [13]. These are just a few points exemplifying the complexity and dynamism of the legal and regulatory environment.

The issues of data security and privacy, and regulatory requirements and compliance, are relevant for all types of organizations, regardless of organizational size and age [11], or industry sector (e.g., healthcare [14], financial services [15] etc.) For these reasons, organizations need to keep a close eye on their legal and regulatory environments, and the developments within it, to avoid non-compliance and the undesirable effects that are associated with it (e.g., financial, reputational) [6].

2.2. IT governance and the COBIT 2019 framework

The monitoring of (changes in) the legal and regulatory environment, and ensuring regulatory compliance, is said to be an important attention point in the context of IT governance [7, 8]. This is referred to as the 'conformance' perspective of IT governance, which is about the protection of IT business value [9]. This aspect is also highlighted in the definition of IT governance, which can be defined as follows: *"[…] an integral part of corporate governance for which, as such, the board is accountable. It involves the definition and implementation of processes, structures, and relational mechanisms that enable both business and IT stakeholders to execute their responsibilities in support of business/IT alignment, and the creation [performance perspective] and protection [conformance perspective] of IT business value."* [16].

As such, organizations need to strive for an appropriate IT governance approach to be able to keep up with changes in their legal and regulatory environments, and ensure regulatory compliance. The link between IT governance and regulatory compliance is not new. For instance, Damianides [5] presented an IT governance framework for responding to the challenges associated with the passage of the Sarbanes-Oxley (SOX) Act. Hardy [3] discussed how IT governance in general, and the COBIT framework (version 4.0) in specific, can be used to respond to legal, regulatory and compliance challenges. Other authors have discussed the issue of 'IT governance transparency', and how this may be related to (changing) compliance requirements [17-20]. It as such appears that an appropriate IT governance approach is required to ensure regulatory compliance, and that an organization's compliance requirements may have an influence on (the appropriateness of) its IT governance approach.

Attention to IT governance is not limited to academic research. Control Objectives for Information and Related Technology (COBIT) is a best-practices practitioner framework for "enterprise governance and management of IT", developed by ISACA. The latest release of this framework is COBIT 2019 [21], which is aimed at facilitating a more flexible and tailored implementation of effective enterprise governance and management of IT. Central to COBIT 2019 is the COBIT 2019 core model, which identifies 40 governance and management objectives. Each governance or management objective always relates to exactly one, respectively, governance or management process. These processes can as such be leveraged to achieve the governance and management objectives, which ultimately results in effective enterprise governance and management of IT.

COBIT 2019's governance and management objectives (and therefore also its processes) are grouped into five domains. The *Evaluate, Direct, and Monitor (EDM)* domain groups the governance objectives together. The purpose of this domain is for the governing body (i.e., the board of directors) to evaluate strategic options, to direct executive management on the chosen strategic options, and to monitor the achievement of the resulting

strategy. The remaining four domains contain the management objectives. The *Align, Plan, and Organize (APO)* domain deals with the identification of how information and technology can best contribute to the achievement of business objectives. It stipulates the need for an information and technology management framework, and contains specific processes related to IT strategy, enterprise architecture, innovation and portfolio management, and data management. Other important focuses of this domain are the management of budgets and costs, human resources, relationships, service agreements, suppliers, quality, risk, and security. The *Build, Acquire, and Implement (BAI)* domain contributes to realizing the IT strategy through the identification of requirements for IT and managing programs and projects. Other focuses of this domain are managing capacity, organizational change, IT changes, acceptance and transitioning, knowledge, assets, and configurations. The *Deliver, Service, and Support (DSS)* domain deals with service delivery. It focuses on managing operations, service requests and incidents, problems, continuity, security services, and business process controls. Finally, the *Monitor, Evaluate, and Assess (MEA)* domain deals with quality assessment and addresses performance management, monitoring of internal control, regulatory compliance, and assurance [16, 21].

2.3. Conceptual model

While extant literature asserts that the monitoring of changes in the legal and regulatory environment, and subsequently ensuring regulatory compliance, is an important attention point in the context of IT governance [7, 8], empirical research on the link between compliance requirements (as imposed upon organizations by their legal and regulatory environment) and IT governance is not available. Moreover, it remains largely unclear what aspects (e.g., processes) of IT governance are important to enable the 'conformance' perspective of IT governance [9], and as such what aspects of IT governance are important for enabling regulatory compliance in an ever-changing legal and regulatory environment. Therefore, the aim of this paper is to investigate the role of compliance requirements in IT governance implementation. More specifically, this paper empirically investigates if organizations with different compliance requirements exhibit differences at the way in which IT governance is implemented. And, if so, how these differences manifest themselves.

The conceptual model of this research is displayed in Figure 1. The dependent construct, *perceived IT governance implementation level*, is operationalized based on COBIT 2019 (and more specifically the processes as structured over the five process domains). For each of the five process domains (i.e., EDM, APO, BAI, DSS, and MEA), a variable is computed that represents the average perceived implementation level of the processes that belong to that respective domain. The independent construct (or grouping variable), *compliance requirements*, is operationalized by means of a categorical variable with three categories (i.e., low, normal, and high), which each represent a different level of compliance requirements to which an organization may be subject to. This construct is as such based on the COBIT 2019 design factor 'compliance requirements'.

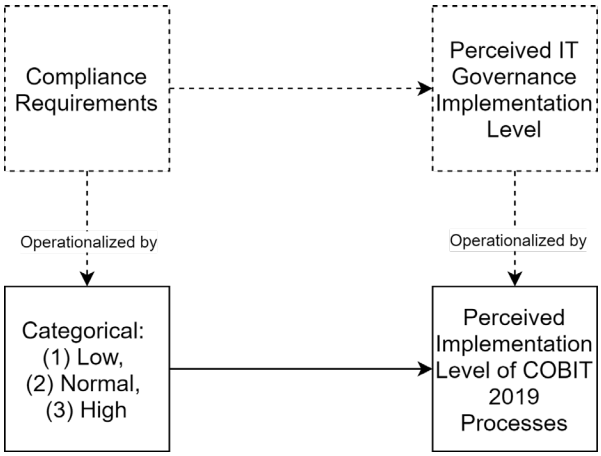

Figure 1. Conceptual model and operationalization

3. Research methodology

3.1. Sample

The dataset on which this research is based was collected by means of an online survey between November 27th, 2020 and December 31st, 2020. Supported by ISACA, business, IT, and governance, risk, and compliance (GRC) representatives were solicited through a global e-mailing campaign. While the descriptions provided in the survey were based on the COBIT 2019 framework, they were expressed in a way that prior knowledge and experience with COBIT 2019 was not required. Among other things, the online survey collected data on the respondents' perceived assessment of the implementation status of the 40 governance and management processes included in the COBIT 2019 framework, as well as the level of compliance requirements to which the organization is subject to. The survey received 3170 responses in total, out of which 2566 were deemed valid responses for data analysis.

The following tables present some sample demographics. Table 1 presents the distribution of

'compliance requirements', which is the independent variable (or grouping variable) in this analysis. It is a 3-point ordinal variable, coded as low – normal – high. If an organization is subject to low compliance requirements, it is subject to a minimal set of regular compliance requirements that are lower than average. An organization that is subject to normal compliance requirements is subject to a set of regular compliance requirements that are common across different industries. Finally, an organization that is subject to high compliance requirements is subject to higher-than-average compliance requirements, most often related to industry sector or geopolitical conditions. While the sample is skewed towards higher compliance requirements, the overall sample is large enough to allow for meaningful comparisons. Moreover, in recent years, security and privacy related issues have received ample attention by regulators, resulting in an overall increase of compliance requirements and pressures for organizations. Table 2 shows the distribution of 'firm size' in the sample. It shows a balanced distribution between different sizes, from small to very large. Table 3 shows the distribution of 'respondent functional area'. This variable represents the functional viewpoint of the respondent and identifies the following four categories: (1) IT department, (2) business department, (3) governance, risk, and compliance (GRC) department, and (4) other. While the vast majority (i.e., 63.3%) of respondents indicated governance, risk, and compliance (GRC) as their functional area, the overall sample is large enough to allow for meaningful comparisons. Finally, Table 4 shows the distribution of the organization's 'role of IT' in the sample. This classification is based on Nolan & McFarlan [22]. If IT is used in "support mode", IT is not considered to be crucial for the running and continuity of the business processes and services, nor for their innovation. If IT is used in "factory mode", there is considered to be an immediate impact on the running and continuity of the business processes and services when IT fails. However, in such organizations, IT is not seen as a driver for innovating business processes and services. If IT is used in "turnaround mode", IT is seen as a driver for innovating business processes and services. However, such organizations do not (yet) have a critical dependency on IT for the current running and continuity of the business processes and services. Finally, if IT is used in "strategic mode", IT is considered to be critical for both running and innovating the organization's business processes and services. While the vast majority (i.e., 62.2%) of organizations in the sample is using IT in "strategic mode", the overall sample is large enough to allow for meaningful comparisons. Moreover, given the contemporary reality of digitalization and digital transformation, it is not surprising that the majority of organizations are using IT for strategic purposes.

In summary, the sample upon which this research is based provides an acceptable balance in terms of compliance requirements, firm size, respondent functional area, and role of IT.

Table 1. Distribution of 'Compliance requirements' (N=2566)

	Frequency	Percent
Low	139	5.4
Normal	1091	42.5
High	1336	52.1

Table 2. Distribution of 'Firm size' (N=2541)

	Frequency	Percent
Fewer than 50 employees	334	13.0
50-149 employees	196	7.6
150-499 employees	284	11.1
500-1,499 employees	322	12.5
1,500-4,999 employees	386	15.0
5,000-9,999 employees	211	8.2
10,000-14,999 employees	117	4.6
15,000 or more employees	691	26.9

Table 3. Distribution of 'Respondent functional area' (N=2566)

	Frequency	Percent
IT department	566	22.1
Business department	231	9.0
Governance, risk, and compliance (GRC)	1624	63.3
Other	145	5.7

Table 4. Distribution of 'Role of IT' (N=2566)

	Frequency	Percent
Support mode	427	16.6
Factory mode	334	13.0
Turnaround mode	209	8.1
Strategic mode	1596	62.2

3.2. Statistical approach

This paper effectively aims to compare central tendency over the three groups of compliance requirements (i.e., low, normal, and high). For this reason, one-way ANOVA is used herein to determine whether group means are different in the population. The one-way ANOVA tests the null hypothesis H_0: all group

population means are equal (i.e., in our case, $\mu_1 = \mu_2 = \mu_3$). Accordingly, the alternative hypothesis is: H_A: at least one group population mean is different (i.e., they are not all equal). An assumption underlying one-way ANOVA is that the dependent variable should be continuous. However, it is common practice to treat ordinal data as continuous, if the scale of that ordinal variable is equidistant. In our case, the scale (i.e., 5-point ordinal from 'not implemented' to 'fully implemented') was indeed constructed to be equidistant. The one-way ANOVA is an omnibus test, as it does not go into specifics about where the differences between groups lie (if any). To find out which combinations of two groups show a significant difference in terms of the dependent variable, pairwise comparisons are used (i.e., a comparison between two separate groups). In the present paper, Tukey's HSD post hoc tests are used when equality of variances is established, and Games-Howell post hoc tests are used when equality of variances is not established. Both of these post hoc tests evaluate all possible combinations of pairwise comparisons.

4. Results

4.1. Descriptives

Table 5 presents descriptive statistics for the five COBIT 2019 process domains over the three categories of compliance requirements (i.e., low, normal, and high).

Table 5. Descriptive statistics for COBIT 2019 process domains over compliance requirements

		N	Mean	Std. Dev.	Min	Max
EDM	Low	136	3.07	0.96	1	5
	Normal	1086	3.35	0.82	1	5
	High	1334	3.56	0.82	1	5
	Total	2556	3.44	0.84	1	5
APO	Low	139	3.22	0.90	1	5
	Normal	1091	3.47	0.78	1	5
	High	1334	3.63	0.79	1	5
	Total	2564	3.54	0.80	1	5
BAI	Low	139	3.26	0.91	1	5
	Normal	1086	3.46	0.82	1	5
	High	1333	3.61	0.81	1	5
	Total	2558	3.53	0.83	1	5
DSS	Low	139	3.38	0.98	1	5
	Normal	1086	3.62	0.83	1	5
	High	1331	3.79	0.82	1	5
	Total	2556	3.69	0.84	1	5
MEA	Low	138	3.24	1.02	1	5
	Normal	1079	3.53	0.89	1	5
	High	1332	3.74	0.87	1	5
	Total	2549	3.62	0.90	1	5

4.2. One-way ANOVA

As a first step, the null hypothesis of equal perceived implementation level at the level of the five COBIT 2019 process domains between the three categories of compliance requirements is tested. The results of this one-way ANOVA analysis are displayed in Table 6. The Levene test for homogeneity of variances was significant for the EDM domain (p=0.034), the DSS domain (p=0.001), and the MEA domain (p=0.006). As a result, a robust test of equality of means (i.e., Welch test) was used for these process domains, the results of which are displayed in Table 7. Based on these results, we find a significant difference for all five process domains. This indicates a considerable difference in the perceived level of IT governance implementation (at the level of the five COBIT 2019 process domains) between the three categories of compliance requirements. A pairwise comparison analysis was subsequently performed to provide more granular insights.

Table 6. One-way ANOVA results for COBIT 2019 process domains (significance level of 0.05)

		Sum of Squares	df	Mean Square	F	Sig.
APO	Between groups	29.763	2	14.881	23.544	0.000
	Within groups	1618.750	2561	0.632		
	Total	1648.513	2563			
BAI	Between groups	23.258	2	11.629	17.285	0.000
	Within groups	1718.965	2555	0.673		
	Total	1742.224	2557			

Table 7. Robust tests of equality of means (i.e., Welch) for COBIT 2019 process domains (significance level of 0.05)

	Welch Statistic	Df1	Df2	Sig.
EDM	29.907	2	365.464	0.000
DSS	20.530	2	372.809	0.000
MEA	27.865	2	371.007	0.000

4.3. Pairwise multiple comparisons

A pairwise comparison analysis allows us to find out which combinations of two groups (i.e., compliance requirements) show a significant difference in terms of the dependent variable (i.e., the perceived level of IT governance implementation at the level of the five COBIT 2019 process domains). As all of the five process domains returned a significant result on the one-way ANOVA, pairwise multiple comparisons are performed for all domains. The results are displayed in the following tables (Table 8 to 12). As the Levene test for homogeneity of variances returned a significant result for the EDM domain (p=0.034), the DSS domain (p=0.001), and the MEA domain (p=0.006), Games-Howell post hoc tests were used for these three domains.

Table 8. Pairwise comparisons for EDM (Games-Howell)

Group Comparison	Mean diff.	Std. Error	Sig.
Low-Normal	-0.279	0.086	0.004
Low-High	-0.486	0.085	0.000
Normal-High	-0.207	0.034	0.000

Table 9. Pairwise comparisons for APO (Tukey HSD)

Group Comparison	Mean diff.	Std. Error	Sig.
Low-Normal	-0.259	0.072	0.001
Low-High	-0.413	0.071	0.000
Normal-High	-0.154	0.032	0.000

Table 10. Pairwise comparisons for BAI (Tukey HSD)

Group Comparison	Mean diff.	Std. Error	Sig.
Low-Normal	-0.200	0.074	0.019
Low-High	-0.347	0.073	0.000
Normal-High	-0.147	0.034	0.000

Table 11. Pairwise comparisons for DSS (Games-Howell)

Group Comparison	Mean diff.	Std. Error	Sig.
Low-Normal	-0.239	0.087	0.017
Low-High	-0.410	0.086	0.000
Normal-High	-0.170	0.034	0.000

Table 122. Pairwise comparisons for MEA (Games-Howell)

Group Comparison	Mean diff.	Std. Error	Sig.
Low-Normal	-0.284	0.091	0.006
Low-High	-0.497	0.090	0.000
Normal-High	-0.213	0.036	0.000

As all pairwise comparisons are significant, the results reveal that the perceived level of IT governance implementation differs significantly between all three categories of compliance requirements. This is true for all five COBIT 2019 process domains. Moreover, we observe that the perceived IT governance implementation level always goes up with increasing compliance requirements. To make our findings more

concrete, we will discuss some key empirical observations in the next section.

4.4. Key observations and discussion

Upon analysis of the survey data regarding the role of compliance requirements in IT governance implementation, three key observations are made:

1. IT governance implementation level (over five different domains) consistently goes up with increasing compliance requirements.
2. Out of the five process domains, 'delivery, service, and support'-related processes appear to be of primary importance, regardless of the level of compliance requirements.
3. There is a relatively stable set of IT governance processes that is important for all compliance requirements levels, although some processes become much more important for the higher levels of compliance requirements.

These observations are discussed in more detail below.

Key Observation 1 – IT governance implementation level (over five different domains) consistently goes up with increasing compliance requirements

Figure 2 shows that for each process domain, the IT governance implementation level increases with increasing compliance requirements. Based on our one-way ANOVA analysis and related post hoc tests, we already know that all of these jumps in IT governance implementation level are statistically significant.

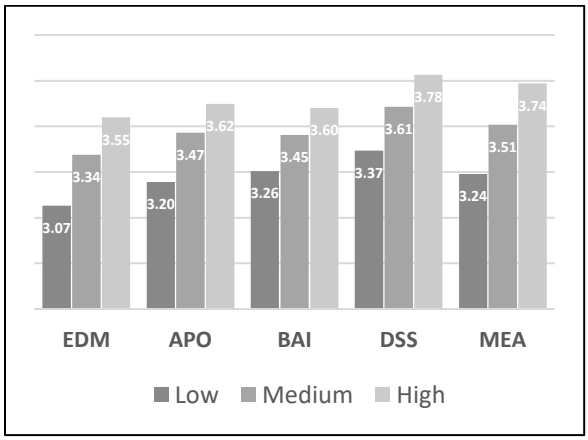

Figure 2. Average IT governance implementation level per process domain, for each level of compliance requirements

We raise some plausible explanations for this observation. First, compliance requirements themselves – due to contents of their actual requirement statements – require that in order to be fulfilled, more mature IT governance and management processes are put in place by the organizations subject to the compliance requirements. Second, compliance requirements very often require that organizations can demonstrate actual compliance, which implies better defined, documented and controlled processes; these are all characteristics of higher maturity levels when referring to the most commonly used process maturity models (i.e., CMMI, ISO/IEC 33000). In our research, the perceived implementation level of the IT governance processes can be considered to be a proxy of the maturity of these processes.

Our observation is also consistent with the key findings of Panetta et al. [17], who investigated (transparency about) IT governance in the European banking sector. They observed a consistently growing attention from banks and regulators for IT Governance starting from 2013, finding a significant effect of regulators' behaviour on banks' behaviour. More specifically, they asserted that the more regulators talked about IT-related issues, the more attention banks paid to IT Governance.

Key Observation 2 – Out of the five process domains, 'delivery, service, and support'-related processes appear to be of primary importance, regardless of the level of compliance requirements.

Figure 3 shows that, out of the five process domains, the 'delivery, service, and support'-related processes (DSS) appear to be of primary importance, regardless of the level of compliance requirements that organizations are subject to. We also note that, the higher the level of compliance requirements, the more important the 'monitor, evaluate, and assess'-related processes (MEA) appear to become. Finally, we observe that the relative difference between the process domain with the highest average implementation level and the one with the lowest average implementation level within a compliance requirement category gets smaller with increasing compliance requirements levels.

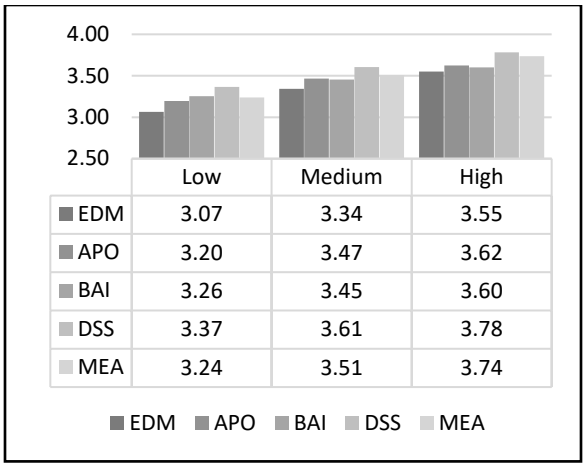

Figure 3. Average IT governance implementation level per level of compliance requirements, for each process domain

We raise some plausible explanations for this observation. The DSS domain encompasses the more operational IT management processes, including continuity and security processes. The MEA domain contains the processes dealing with performance and conformance monitoring, internal control, external compliance, and assurance. With this in mind, we first note that the actual requirements contained in many contemporary IT regulations often deal with privacy, security, continuity and business controls, which are thus mostly achieved through the processes contained in the DSS domain. Second, as the MEA domain contains compliance-related processes, it makes perfect sense that for higher compliance requirements these processes tend to have a higher implementation level. This also explains why the difference between implementation level of the DSS domain and the MEA domain almost disappears with increasing compliance requirements levels, as compliance-related processes logically become more important under high compliance requirements.

Key Observation 3 – A relatively stable set of IT governance processes that is important for all compliance requirements levels

We identified the processes that belong to the fourth quartile (i.e., top 25%) for each compliance requirements level, in terms of their perceived implementation level. The goal of this analysis is to identify what IT governance processes are important under different levels of compliance requirements, and evaluate any differences. The result of this analysis is shown in Figure 4, where implementation levels highlighted in grey belong to the fourth quartile (i.e., top 25%) of processes for the respective level of compliance requirements.

	Low	Normal	High
DSS01	3.55	3.66	3.84
MEA03	3.46	3.66	3.92
DSS02	3.39	3.69	3.85
APO06	3.49	3.62	3.77
DSS04	3.39	3.60	3.84
DSS05	3.35	3.62	3.84
APO13	3.33	3.62	3.83
BAI11	3.40	3.55	3.67
BAI06	3.31	3.54	3.74
DSS03	3.30	3.57	3.69
BAI04	3.31	3.51	3.70
EDM05	3.31	3.52	3.68
APO11	3.40	3.53	3.62
APO09	3.26	3.55	3.66
MEA04	3.23	3.50	3.74
APO07	3.39	3.49	3.64

Figure 4. Top 25% of IT governance processes per level of compliance requirements

We raise some interesting observations and plausible explanations. First, in line with the previous key observation, almost all DSS processes are represented in the top 25% of processes (in terms of perceived implementation level). The importance of the DSS processes in light of the actual requirements contained in many contemporary IT regulations was already discussed as part of the previous key observation. Second, five processes are consistently in the top 25% of processes, regardless of the level of compliance requirements, i.e., DSS01 on *managing IT operations*, MEA03 on *managing external compliance*, DSS02 on *managing service requests and incidents*, APO06 on *managing budget and costs*, and DSS04 on *managing continuity*. These processes thus form a stable set that appears to be important for all compliance requirements levels. It should be noted that two additional processes are added to this list for the normal and high compliance requirements levels, i.e., DSS05 on *managing security services*, and APO13 on *managing security*. In other words, for normal and high compliance requirements levels, security related issues appear to become highly important. Finally, given that the MEA domain contains compliance-related processes, it is not surprising that these processes become more important with higher

compliance requirements levels. While MEA03 on *managing external compliance* is part of the stable set of processes that appears to be important for all compliance requirements levels, MEA04 on *managing assurance* becomes part of the top 25% of processes for those organizations that are subject to the highest level of compliance requirements. This process is about planning, scoping and executing assurance initiatives to comply with internal requirements, laws, and regulations.

4.5. Contribution

The results of this research contribute to literature by means of providing empirical evidence related to the 'conformance' perspective of IT governance. More specifically, we shed light on the role of compliance requirements in IT governance implementation, and on what IT governance processes appear to be important under different levels of compliance requirements. As such, we also explore an organization's legal and regulatory environment, and more specifically the compliance requirements imposed by this environment, as a contingency factor for IT governance.

In terms of practical contribution, organizations can use the results of this research for external benchmarking purposes. Our concrete insights on the IT governance processes that appear to be important in different legal and regulatory environments (i.e., environments with different compliance requirements) may enable organizations to evaluate if their approach to IT governance is appropriate, given the level of compliance requirements that they are subject to. Our results indicate that compliance requirements are positively related to IT governance implementation level. As such, if the legal and regulatory environment of an organization becomes more complex, the organization may be in need of a more mature IT governance implementation.

4.6. Limitations and future research opportunities

In this section, we discuss some limitations and future research opportunities related to our research. First, we acknowledge that our research focused on the *perceived* IT governance implementation level. In other words, our analysis was based on perception data. While it is certainly not feasible to collect a dataset of this size by independently assessing the real situation in terms of IT governance implementation level, this potential source of bias should be acknowledged. Second, we identified some imbalances in our sample in terms of compliance requirements (i.e., the grouping variable in our one-way ANOVA analysis). More specifically, the group of organizations subject to *low* compliance requirements (N=139) is much smaller than the group of organizations subject to *normal* (N=1091) and *high* (N=1336) compliance requirements. While the overall sample is large enough to allow for meaningful comparisons, we acknowledge that the statistical power of comparing the *low* group to the *normal* or *high* group is lower than comparing the *normal* group to the *high* group. Third, we acknowledge that this research limited itself to focusing on the "what" of the role of compliance requirements in IT governance implementation, not the "how" and "why". As such, future research may focus on investigating the "how" and "why" more in-depth, e.g., by means of case study research. Finally, we would like to acknowledge the question of causality. Although we observe a clear positive correlation between IT governance implementation level and compliance requirements, we cannot claim the direction of causality based on our analysis. However, we do suspect that higher compliance requirements are a trigger for higher IT governance implementation levels, notwithstanding the often-made comment that many organizations subject to compliance requirements do not see this as a value-adding activity, and therefore try to do the minimum required to comply. Future research may also further investigate this aspect, related to the difference between the 'conformance' and 'performance' perspectives of IT governance.

5. Conclusion

This paper investigated if organizations with different compliance requirements exhibit differences at the way in which IT governance is implemented. And, if so, how these differences manifest themselves. Based on a large and diverse sample of organizations (N=2566), our results indicated that IT governance implementation level (over five different process domains) consistently goes up with increasing compliance requirements, and that these jumps in IT governance implementation level are always statistically significant. Moreover, we observed that there is a relatively stable set of IT governance processes that is important for all compliance requirements levels, of which especially the 'delivery, service, and support'-related processes appear to be crucial aspects. Finally, we also found that, for the higher compliance requirements, security and

assurance related processes appear to become much more important.

References

[1] G. Vial, "Understanding digital transformation: A review and a research agenda," *The Journal of Strategic Information Systems,* vol. 28, no. 2, pp. 118-144, 2019.

[2] P. Soto-Acosta, "COVID-19 pandemic: Shifting digital transformation to a high-speed gear," *Information Systems Management,* vol. 37, no. 4, pp. 260-266, 2020.

[3] G. Hardy, "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges," *Information Security technical report,* vol. 11, no. 1, pp. 55-61, 2006.

[4] E. Karanja and J. Zaveri, "Ramifications of the Sarbanes Oxley (SOX) Act on IT governance," *International Journal of Accounting and Information Management,* 2014.

[5] M. Damianides, "Sarbanes-Oxley and IT governance: New guidance on IT control and compliance," *Information Systems Management,* vol. 22, no. 1, pp. 77-85, 2005.

[6] D. Gozman and L. Willcocks, "The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations," *Journal of Business Research,* vol. 97, pp. 235-256, 2019.

[7] R. Singh, A. Baird, and L. Mathiassen, "Ambidextrous governance of IT-enabled services: A pragmatic approach," *Information and Organization,* vol. 30, no. 4, 2020, Art no. 100325.

[8] T. Huygh and S. De Haes, "Towards a Viable System Model-based Organizing Logic for IT Governance," in *ICIS 2020*, Hyderabad, India, 2020.

[9] D. Smits and J. van Hillegersberg, "Hard and Soft Governance: The Missing Link Between Corporate and IT Governance," in *Proceedings of the 6th International Conference on Management, Leadership and Governance*, V. Ribiere Ed., (Proceedings of the International Conference on Management Leadership and Governance, 2018, pp. 421-430.

[10] T. Butler and D. McGovern, "A conceptual model and IS framework for the design and adoption of environmental compliance management systems," (in English), *Information Systems Frontiers,* Article vol. 14, no. 2, pp. 221-235, 2012.

[11] C. Norval, H. Janssen, J. Cobbe, and J. Singh, "Data protection and tech startups: The need for attention, support, and scrutiny," *Policy and Internet,* 2019.

[12] K. Brandis, S. Dzombeta, R. Colomo-Palacios, and V. Stantchev, "Governance, Risk, and Compliance in Cloud Scenarios," *Applied Sciences-Basel,* vol. 9, no. 2, 2019, Art no. 320.

[13] European Commission, "Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," 2021.

[14] C. Thapa and S. Camtepe, "Precision health data: Requirements, challenges and existing techniques for data security and privacy," *Computers in Biology and Medicine,* vol. 129, 2021, Art no. 104130.

[15] O. Akanfe, R. Valecha, and H. R. Rao, "Assessing country-level privacy risk for digital payment systems," *Computers & Security,* vol. 99, 2020, Art no. Pmid 102065.

[16] S. De Haes, W. Van Grembergen, A. Joshi, and T. Huygh, *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations, Third Edition*. Cham, Switzerland: Springer, 2020.

[17] I. C. Panetta, S. Leo, F. Santoboni, and G. Vento, "IT governance in the banking sector: Evidence from Italy, Germany, France and Spain," *Economic Review: Journal of Economics and Business,* vol. 15, no. 2, pp. 63-76, 2017.

[18] S. De Haes, T. Huygh, and A. Joshi, "Exploring the Contemporary State of Information Technology Governance Transparency in Belgian Firms," *Information Systems Management,* vol. 34, no. 1, pp. 20-37, 2017.

[19] S. De Haes, T. Huygh, A. Joshi, and L. Caluwe, "National Corporate Governance Codes and IT Governance Transparency in Annual Reports," *Journal of Global Information Management,* vol. 27, no. 4, pp. 91-118, 2019.

[20] T. Huygh, S. De Haes, A. Joshi, W. Van Grembergen, and D. Gui, "Exploring the influence of Belgian and South-African corporate governance codes on IT governance transparency," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[21] ISACA, "COBIT 2019: Introduction and Methodology," 2018.

[22] R. Nolan and F. W. McFarlan, "Information technology and the board of directors," *Harvard business review,* vol. 83, no. 10, pp. 1-10, 2005.